Application No. 10/000,396
Reply to Office Action of September 15, 2005
Page 5 of 25

CLAIMS

This listing of claims will replace all prior version and listings of claims in the application:

1. (Currently amended) A method of analyzing network communication traffic on a data communication network for determining whether the traffic is legitimate or potential suspicious intrusion activity, comprising the steps of:

monitoring packets exchanged between two hosts on the data communication network;

identifying a flow corresponding to a predetermined plurality of packets exchanged between the two hosts that relate to a single service and is delimited by a predetermined event assigning packets to a flow;

collecting flow data from packet headers;

assigning analyzing collected flow data to assign a concern index value to an identified the flow based upon a probability predetermined characteristic of that the flow was not normal for data communications;

maintaining an accumulated concern index comprising concern index values for one or more identified from flows associated with a host; and

issuing an alarm signal once in the event that the accumulated concern index has exceeded for a host exceeds an alarm threshold value.

2. (Currently amended) The method of claim 1, wherein the predetermined event for delimiting a flow is selected from the group comprising the elapse of a predetermined period of time wherein no packets are exchanged between two hosts, the occurrence of a FIN flag, predetermined characteristics of traffic on a given port, and the occurrence of a RESET packet the flow consists of the packets exchanged between two hosts that are associated with a single service.

1370936 v03

3.   (Currently amended) The method of claim 1, <u>further comprising the step of</u> <u>communicating a message to a firewall to drop packets going to or from the</u> <u>particular host in response to</u> ~~wherein~~ the alarm signal ~~updates a firewall for~~ ~~filtering packets transmitted by a host~~.

4.   (Currently amended) The method of claim 1, wherein the alarm signal generates a notification to <u>a</u> ~~the~~ network administrator.

5.   (Currently amended) The method of claim 1, wherein each concern index value associated with a <u>predetermined event</u> ~~respective potential intrusion activity~~ is a predetermined fixed value.

6.   (Currently amended) A method of analyzing network communication traffic <u>on a</u> <u>data communication network</u> for <u>determining whether the traffic is legitimate or</u> potential <u>suspicious</u> ~~intrusion~~ activity, comprising the steps of:
          <u>monitoring packets exchanged between two hosts that are</u> <u>associated with a single service on the data communications network;</u>
          <u>identifying a flow corresponding to a predetermined plurality of</u> ~~assigning packets to a flow, wherein a flow consists of the~~<u>packets</u> exchanged between <u>the</u> two hosts ~~that are associated with a single service~~;
          collecting flow data from packet headers <u>of the packets in the</u> <u>identified flow;</u>
          <u>based on the collected flow data, assigning</u> ~~analyzing collected~~ ~~flow data to assign~~ a concern index value <u>to the flow based on a</u> <u>predetermined characteristic of the flow</u> ~~wherein each concern index value~~ ~~associated with a respective potential intrusion activity is a predetermined~~ ~~fixed value~~;

maintaining an accumulated concern index from flows that are associated with a particular host; ~~and~~

issuing an alarm signal in the event that ~~once~~ the accumulated concern index for the particular host exceeds ~~has exceeded~~ an alarm threshold value; and

in response to the alarm signal, sending a message to a utilization component.

7.   (New) (NOTE: NO CLAIM PRESENTED FOR CLAIM 7 IN ORIGINAL APPLICATION DUE TO TYPOGRAPHICAL ERROR) The method of claim 6, wherein the utilization component is selected from the group comprising: network security device, email, SNMP trap message, beeper, cellphone, firewall, network monitor, user interface display to an operator.

8.   (Currently amended) A method of analyzing network communication traffic on a data communication network for determining whether the traffic is legitimate or potential suspicious ~~intrusion~~ activity, comprising the steps of:

monitoring the exchange of packets between two hosts each having a particular Internet Protocol (IP) address;

identifying a flow corresponding to a predetermined plurality of packets exchanged between a particular port of one of the hosts that remains constant during the plurality of packets ~~assigning packets to a flow, wherein a flow consists of the packets exchanged between two Internet Protocol addresses with at least one port remains constant~~;

collecting flow data from packet headers of the packets in the identified flow;

based on the collected flow data, assigning ~~analyzing collected flow data to assign~~ a concern index value to the flow;

maintaining a host <u>data</u> structure containing ~~an~~ accumulated concern index <u>values</u> from <u>a plurality of</u> flows <u>that are</u> associated with the <u>particular</u> host; and

issuing an alarm <u>in the event that</u> ~~once~~ the accumulated concern index <u>values for the particular host</u> has exceeded an alarm threshold value.

9. (Currently amended) The method of claim 8, wherein each concern index value associated with a respective potential <u>suspicious</u> ~~intrusion~~ activity is a predetermined fixed value.

10. (Currently amended) A system for analyzing network communication traffic <u>and</u> <u>determining potential suspicious activity</u>, comprising:

~~a computer system operable to classify packets into flows, collect flow data from packet header information, analyze collected flow data to assign a concern index value wherein each concern index value associated with a respective potential intrusion activity is a predetermined fixed value, and generate an alarm signal;~~

<u>a computer system operative to:</u>

a) <u>monitor the communication of packets on a data communication network;</u>

b) <u>classify the monitored packets into flows, wherein a flow corresponds to a predetermined plurality of packets exchanged between two hosts that are associated with a single service on the network;</u>

c) <u>analyze the flows in order to assign a concern index value to a flow that may signify potential suspicious activity, wherein each concern index value associated with a respective potential suspicious activity is of a predetermined fixed value;</u>

d) <u>generate an alarm signal in response to cumulated concern index values; and</u>

1370936 v03

Application No. 10/000,396
Reply to Office Action of September 15, 2005
Page 9 of 25

a communication system coupled to the computer system <u>operative to</u>
<u>receive packets communicated between hosts on the network</u> ~~operable to send~~
~~packets from one host to another host.~~

11.　　(Currently amended) A system for analyzing network communication traffic <u>and</u>
<u>determining potential suspicious activity</u>, comprising:

~~a processor operable to classify packets into flows, collect flow data from~~
~~packet header information, analyze collected flow data to assign a concern~~
~~index value wherein each concern index value associated with a respective~~
~~potential intrusion activity is a predetermined fixed value, and generate an~~
~~alarm signal;~~

<u>a processor operative to:</u>

　　<u>a)</u>　　<u>monitor the communication of packets on a data</u>
　　　　<u>communication network;</u>

　　<u>b)</u>　　<u>classify the monitored packets into flows, wherein a flow</u>
　　　　<u>corresponds to a predetermined plurality of packets</u>
　　　　<u>exchanged between two hosts that are associated with a</u>
　　　　<u>single service on the network;</u>

　　<u>c)</u>　　<u>maintain a flow data structure for storing data</u>
　　　　<u>corresponding to a plurality of flows;</u>

　　<u>d)</u>　　<u>analyze the flows in the flow data structure in order to</u>
　　　　<u>assign a concern index value to a flow that may signify</u>
　　　　<u>potential suspicious activity, wherein each concern index</u>
　　　　<u>value associated with a respective potential suspicious</u>
　　　　<u>activity is of a predetermined fixed value;</u>

　　<u>e)</u>　　<u>cumulate assigned concern index values of one or more</u>
　　　　<u>flows associated with a particular host;</u>

1370936 v03

    f)   maintain a host data structure for storing data associating a cumulated concern index value with each one of a plurality of hosts; and

    g)   generate an alarm signal in response to cumulated concern index values in the host data structure;

a memory coupled to the processor and operative ~~operable~~ to store the flow data structure and the host data structure ~~the flow data~~;

~~a database coupled to processor operable to store log files;~~ and

a network interface coupled to the processor operative to receive packets on the data communication network ~~operable to monitor network traffic~~.

12.   (Currently amended) A method of analyzing network communication traffic on a data communication network for potential suspicious ~~intrusion~~ activity, comprising the steps of:

    monitoring packets exchanged between two hosts on the data communication network;

    ~~analyzing packet header information;~~

    identifying packets provided by one of the two hosts that have ~~determining~~ a transport level protocol specifying a packet format that includes a data segment ~~of a data area~~ ;

    in response to determination that the transport level protocol is a User Datagram Protocol (UDP) packet and the data segment associated with the UDP packet contains two bytes or less of data, storing a concern index value of a predetermined amount in a memory in association with information identifying the host that issued the UDP packet; and

    issuing an alarm when the cumulated concern index value associated with the host exceeds a predetermined threshold level ~~transport level protocol is identified as User Datagram Protocol (UDP) and the data~~

~~segment associated with User Datagram Protocol packet contains two or less bytes of data.~~

13. (New) The method of claim 6, wherein a flow is determined as terminated in response to a predetermined event selected from the group comprising the elapse of predetermined period of time where no packets are exchanged between two hosts, the occurrence of a FIN flag, predetermined characteristics of traffic on a given port, and the occurrence of a RESET packet.

14. (New) The method of claim 8, wherein a flow is determined as terminated in response to a predetermined event selected from the group comprising the elapse of a predetermined period of time wherein no packets are exchanged between two hosts, the occurrence of a FIN flag, predetermined characteristics of traffic on a given port, and the occurrence of a RESET packet.

15. (New) The system of claim 10, wherein a flow is determined as terminated in response to a predetermined event selected from the group comprising the elapse of a predetermined period of time wherein no packets are exchanged between two hosts, the occurrence of a FIN flag, predetermined characteristics of traffic on a given port, and the occurrence of a RESET packet.

16. (New) The system of claim 11, wherein a flow is determined as terminated in response to a predetermined event selected from the group comprising the elapse of a predetermined period of time wherein no packets are exchanged between two hosts, the occurrence of a FIN flag, predetermined characteristics of traffic on a given port, and the occurrence of a RESET packet.

17. (New) The method of claim 1, wherein the single service comprises a port number remaining constant for a plurality of packets.

1370936 v03

Application No. 10/000,396
Reply to Office Action of September 15, 2005
Page 12 of 25

18.   (New) The method of claim 1, wherein the suspicious activity is from an inside
       address or from an outside address.

19.   (New) The method of claim 1, wherein the concern index for a suspicious
       activity is derived by reference to a table of predetermined suspicious activities
       each having a predetermined concern index value.

20.   (New) The method of claim 1, wherein the host for which the concern index is
       accumulated is an inside host.

21.   (New) The method of claim 1, wherein the host for which the concern index is
       accumulated is an outside host.

22.   (New) The method of claim 1, wherein the steps are carried out in a monitoring
       appliance.

23.   (New) The method of claim 22, wherein the monitoring appliance is installed
       behind a firewall.

24.   (New) The method of claim 22, wherein the monitoring appliance is connected
       before a firewall.

25.   (New) The method of claim 22, wherein the monitoring appliance is connected in
       a DMZ.

26.   (New) The method of claim 22, wherein the monitoring appliance is configured
       to operate as a pass-by filter.

1370936 v03

Application No. 10/000,396
Reply to Office Action of September 15, 2005
Page 13 of 25

27. (New) The method of claim 22, wherein the monitoring appliance is coupled to a network device.

28. (New) The method of claim 27, wherein the network device is selected from group comprising: router, switch, hub, tap.

29. (New) The method of claim 27, wherein the network device is a network security device.

30. (New) The method of claim 1, wherein the monitoring of packets comprises monitoring on packet header information only.

31. (New) The method of claim 1, wherein the monitoring of packets is carried out in a device operating in a promiscuous mode.

32. (New) The method of claim 1, wherein the alarm signal is provided to a utilization component.

33. (New) The method of claim 32, wherein the utilization component is selected from the group comprising: network security device, email, SNMP trap message, beeper, cellphone, firewall, network monitor, user interface display to an operator.

1370936 v03